

Primo Piano - *Sicurezza informatica, falla in Claude Code: oltre mille password aziendali e 100mila documenti finiti sul web*

Roma - 10 nov 2026 (Prima Notizia 24) **Scoperto dalla società Apiiro un bug legato alla memorizzazione automatica delle autorizzazioni dell'assistente IA di Anthropic. I dati sensibili sono stati pubblicati su GitHub, la società al lavoro per risolvere il problema.**

Una falla nei sistemi di sicurezza legati all'intelligenza artificiale ha portato alla pubblicazione in rete di centinaia di dati sensibili, tra cui oltre mille password e credenziali aziendali riservate. A individuare la vulnerabilità è stata la società di sicurezza informatica Apiiro, che ha rintracciato la diffusione incolpevole di informazioni private sulla piattaforma per sviluppatori GitHub. All'origine dell'incidente vi è Claude Code, l'assistente per programmatori sviluppato da Anthropic, progettato per operare in autonomia sugli elaboratori eseguendo cicli continuativi di lettura, pianificazione, azione e verifica senza la necessaria supervisione costante dell'utente. Stando alle ricostruzioni degli esperti, il malfunzionamento è scaturito dal meccanismo di memorizzazione delle preferenze dell'utente, in particolare dall'opzione che consente di autorizzare le operazioni evitando future richieste di conferma. Per registrare tale scelta, il programma genera un file locale sul computer, procedura che si applica anche quando le informazioni da conservare comprendono chiavi d'accesso o codici di servizio. Quando tale file viene successivamente copiato su un altro dispositivo o riconfigurato, le restrizioni previste per impedire la condivisione online tendono a disattivarsi a causa di un errore di sistema, determinando il caricamento automatico dei file su repository pubblici. L'indagine condotta da Apiiro ha conteggiato oltre 100mila documenti pubblicati da Claude Code sul web, in più di un migliaio dei quali erano direttamente visibili codici di accesso e password private. Il quadro è reso ulteriormente complesso dal fatto che, una volta caricati in rete, i dati restano indicizzati e visibili anche in caso di successiva rimozione del file originale dal computer locale. Gli sviluppatori di Anthropic hanno reso noto di aver avviato le procedure per la risoluzione del bug e per l'implementazione di correttivi volti a prevenire il ripetersi del problema.

(Prima Notizia 24) Martedì 10 Novembre 2026